정 보 보 호 학 회 지
제28권 제6호, 2018. 12

방산보안 2.0

류 연 승*

요 약

방산보안은 방위산업과 관련된 보안으로 방위산업의 발전에 따라 방산보안의 정의도 변화되어왔다. 우리나라 방위산업은 1970년대에 본격적으로 육성되었고 방산보안은 군사기밀을 취급하며 방산물자를 생산하는 방위산업체의 보안으로 정의되어왔다. 최근 무기체계 및 핵심기술의 국제공동연구개발에 따른 도입 기술의 보호가 필요하고, 선진국 수준에 이른 국방과학기술을 이용한 방산물자의 수출이 증가하면서 방위산업기술을 보호하기 위한 방위산업기술보호법이 제정되었다. 방산보안의 역사를 살펴볼 때 큰 전환점이 도래하는 것이며 방산보안 시대를 구분하고 각 시대의 특징을 정리해보는 것이 의미가 있다. 본 논문에서는 방위산업기술보호법 제정 이후를 방산보안 2.0 시대로 규정하고, 시대 별 주요 특징을 비교하며 향후 발전방향을 고찰하였다.

Ⅰ. 서 론

우리나라는 해방 후 60년대 까지 주로 미국의 군원에 의존하여 군사력을 유지해왔고, 70년대에 자주국방 추진으로 국방과학연구소 창설 및 중화학공업 육성과 함께 본격적으로 방위산업이 육성되었다[1,2]. 방위산업의 발전은 국가적으로 철강, 기계, 화학, 자동차, 조선, 전자산업이 세계적인 수준으로 발전해온 것과 맥락을 같이 한다. 방위산업의 발전 단계를 보면 정부 주도의 보호·육성 및 기반 구축 단계, 경쟁 및 자립 발전 단계, 그리고 국제경쟁력 확보 및 세계시장 진출 단계로 나누어 볼수 있다[1].

현재 우리나라 방위산업은 보호·육성 단계에서 벗어나 경쟁 및 자립 발전 단계에 접어든 수준이고 일부 앞서 나가는 분야는 국제경쟁력을 갖추기 위한 수준에 진입하고 있다. 1990년대부터 한국형 무기체계 개발을 추진해온 결과, 전차, 장갑차, 구축함, 초계함, 잠수함, 고속정, 유도무기, 통신·전자전 장비, 훈련기와 전투기에 이르기까지 최첨단 무기체계를 독자개발하고 있다. 최근에는 무기체계의 해외 수출도 크게 증가하고 있는데 K9 자주포, K2 전차, FA-50 경공격기, T-50 훈련기, 209급 잠수함, 군수지원함 등은 대표적인 수출 품목으로 2017년 방산수출액은 약 31억불에 이르렀다. 또한, 국방기술품질원이 2015년에 발간한 국방과학기술수준조사서에 의하면, 국방과학기술의 전반적인 수준은 선진국 미국 대비 80% 수준으로 세계 9위권의 수준으로 평가되고 있다.

방산업체의 보안은 방위산업의 초기인 1960년대부터 시작되어 방산물자를 생산·공급하는 방산업체의 기밀을 보호하고, 업체가 방산물자를 적절한 시기에 생산·공급할 수 있도록 지원하는 제반 활동으로서 국방보안의 일환으로 운용되어 왔다. 정부가 지정하는 방산업체는 국가 안보를 위해 보호해야 하는 군사기밀을 취급하고 있기 때문에 국방부가 제정한 「방위산업보안업무훈령」에 따른 보안 체계를 갖추고 매년 보안감사를 받고 있다[3].

최근 방산물자의 수출이 증가하고 선진국 수준에 이른 국방과학기술 보호의 필요성이 증대되면서 방위사업청은 2015년 말 「방위산업기술보호법」을 제정하였다[4]. 세계적 수준의 우수한 국방과학기술이 해외로 유출된다면 국가 안전보장과 국가경제에 피해를 주며 국제평화에도 저해요소로 작용할 수 있으므로 국방과학기술의 보호가 필요하다.

방위산업기술보호법의 시행과 더불어 방산보안 관련된 법, 제도가 변화하고 정보통신 등의 기술 발달로 인해 방산보안 환경이 크게 변화하고 있다. 방산보안의 역사를 살펴볼 때 큰 전환점이 도래하는 것으로 판단되며 이에 방산보안 시대를 구분하고 각 시대의 특징과 향후

* 명지대학교 보안경영공학과 교수 (ysryu@mju.ac.kr)

과제를 정리해보는 것이 의미가 있다. 본 논문에서는 방위산업기술보호법 제정 이후를 방산보안 2.0 시대로 규정하고 이전 1.0 시대와의 특징을 비교하여 살펴봄으로써 향후 과제를 제시해본다.

Ⅱ. 방산보안 역사

방위산업이 태동하는 초기의 방위산업 보안은 군에 필요한 각종 장비 및 장병들의 의식주에 필요한 물품을 생산하는 업체가 파업이나 화재 등 각종 사고시 군에 직접적 피해가 올 수 있어 이를 예방하기 위한 제도이었다. 이후 방위산업 보안은 적(불순분자)으로부터 군이 필요로하는 방산물자를 생산·공급하는 방산업체의 기밀을 보호하고, 업체가 방산물자를 적절한 시기에 생산·공급할 수 있도록 지원하도록 보장하기 위한 제반 활동으로 정의되었다. 이러한 활동에는 적(불순분자)의 간첩 행위나 태업 등으로부터 방산업체가 보유하고 있는 유·무형 자산(기술, 인력, 장비, 정보 등)을 보호하고 손실을 방지하기 위한 보안 활동을 포함하였다.

제도적인 역사를 살펴보면, 1965년 국방부는 「군사보안업무훈령」에 의해 군수업체 보안 업무를 수행하였고 1966년 군수 공장 및 군납업체 대상으로 보안측정 결과를 계약체결 시 반영하였다. 1977년에 국방부 훈령인 「방위산업보안업무훈령」이 제정되면서 군수업체에 대한 방위산업보안업무 지원체제가 마련되어 오늘에 이르고 있다.

방산업체로 지정받으려면 대통령령이 정하는 시설기준과 보안요건을 갖추어야 한다. 구축해야 할 보안요건은 방위사업법 시행령에 규정되며 방위산업보안업무훈령으로 상세하게 제시된다. 방위사업법 제3조 및 제35조에 의해 방산업체의 정의를 살펴보면 “방산물자를 생산하는 업체로서 대통령령이 정하는 시설기준과 보안요건 등을 갖추어 산업통상자원부 장관으로부터 지정받은 업체”로 정의된다[5]. 본 정의에 명시된 “보안요건”이란 방위사업법 시행령 제44조에 그림 1과 같이 규정되어 있다.

이러한 보안요건은 군사기밀을 취급하는 방산업체의 기밀 유출을 방지하기 위한 보안체계 요건을 일컫는 것이다. 국방부는 방산업체의 보안 업무를 지원하기 위해 방위산업보안업무훈령을 제정하였고, 방산업체는 이 훈령에 따라 방위사업법에 규정된 보안 요건의 보안 대책을 운용해야 한다. 국방부는 매년 보안감사를 통해 방산업체의 보안 대책을 점검하고 기밀 유출 예방 활동을 하고 있다. 방위산업보안업무훈령의 주요 내용은 계획보안, 문서보안, 기업보안, 인원보안, 시설보안, 정보통신보안 등으로 구성된다.

제44조(보안요건 및 측정 등) ①법 제35조제1항의 규정에 의한 보안요건은 다음 각 호와 같다.
1. 방산시설이 충분히 보호될 수 있는 지역 및 시설에 관한 보안대책
2. 방산업체에 종사하는 인원에 관한 보안대책
3. 비밀문서의 취급 및 보관·관리에 관한 보안대책
4. 방산물자 및 원자재에 관한 보호대책
5. 장비 및 설비의 보호대책
6. 통신시설 및 통신수단에 대한 보안대책
7. 각종 자료의 정보처리과정 및 정보처리 결과자료의 보호대책
8. 보안사고에 대비한 관계정보기관과의 유기적인 통신수단
9. 그 밖에 보안유지를 위하여 방위사업청장이 필요하다고 인정하는 보안대책

〔그림 1〕 방산업체의 보안요건 (출처: 방위사업법 시행령)

한편, 2006년 개청된 방위사업청은 2012년 방산기술통제관실을 신설하였다. 방산기술통제관실은 2015년 12월 방위산업기술보호법을 제정하여 국방과학기술 중 국가안보를 위해 보호해야 하는 기술을 방위산업기술로 지정하고 방산업체 등 대상기관의 방위산업기술 보호체계 구축을 지원하고 있다. 방산기술통제관실은 2018년 11월 핵심기술 기획·개발 조직을 포함하는 국방기술보호국으로 확대개편되었다.

방산업계는 무기체계 및 핵심기술의 국제공동연구개발이 확대되면서 해외에서 도입된 기술도 보호가 요구된다. 또한, 우리나라는 UN 무기거래조약, 다자간 수출통제체제 등 여러 무기거래 관련 국제조약에 가입하고 있으며 국방과학기술의 수출 인허가 제도 운영을 통하여 불법적인 해외 유출을 방지함으로써 세계 평화에 기여하고 있다. 방산업체가 방산물자 또는 국방과학기술을 수출할 때는 승인을 받도록 방위사업법 제57조로 통제하고 있으나, 업체가 보유하고 있는 국방과학기술이 국내외로 유출될 위협에 대해서 업체들이 구축해야 할 기술보호체계에 대한 법적 체계는 미비하였다. 이러한 배경에서 방위사업청은 방위산업기술보호법을 제정하고 141개 기술을 방위산업기술로서 지정 고시하였다. 방위산업기술보호법의 목적은 국방과학기술을 보호하고 관련기관을 지원함으로써 국가의 안전을 보장하고

1. 보호대상 기술의 식별 및 관리 체계: 대상기관이 체계적으로 보호대상 기술을 식별하고 관리하는 체계
   ① 대상기관이 보유하고 있거나 연구개발을 통하여 확보한 기술 중 방위산업기술을 분류·식별하는 체계
   ② 방위산업기술과 관련된 정보를 체계적으로 축적·관리할 수 있도록 하는 인적·물적 체계

2. 인원통제 및 시설보호 체계: 허가받지 않은 사람의 출입·접근·열람 등을 통제하고, 방위산업기술과 관련된 시설을 탐지 및 침해 등으로부터 보호하기 위한 체계
   ① 방위산업기술 보호책임자의 임명, 보호구역의 설정 및 출입 제한을 통한 인원통제 체계
   ② 보호구역에 보안장비 설치를 통한 방위산업기술에 대한 불법적인 접근을 탐지하는 시설보호 체계

3. 정보보호체계: 방위산업기술과 관련된 정보를 안전하게 보호하고, 이에 대한 불법적인 접근을 탐지 및 차단하기 위한 체계
   ① 방위산업기술을 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안 체계
   ② 컴퓨터바이러스 등으로부터 방위산업기술 침해를 방지하기 위한 소프트웨어 설치를 통한 보호 체계
   ③ 방위산업기술 정보에 대한 침입을 탐지·차단하기 위한 방화벽 및 보안관제 시스템 설치를 통한 보호 체계
   ④ 방위산업기술 정보에 접속하는 시스템·컴퓨터 등에 대한 외부망 차단 체계

〔그림 2〕 방위산업기술 보호체계 (출처: 방위산업기술보호법)

국제조약 등의 의무를 이행하여 국가 신뢰도를 제고하기 위한 것이다.

방위산업기술보호법의 적용 대상기관은 국방과학연구소, 방사청, 각군, 국방기술품질원 등의 국방관련기관과 방위산업체 및 전문연구기관, 그 밖에 기업 · 연구기관 · 전문기관 및 대학 등으로 방위산업기술을 보유하거나 방위산업기술과 관련된 연구개발사업을 수행하고 있는 기관이다. 국방관련기관은 국방보안업무훈령에 의한 보안체계를 갖추어야 하고 방산업체는 방위산업보안업무훈령에 의한 보안체계를 갖추어야 한다. 더불어, 방위산업기술보호법의 시행에 따라 방위산업기술을 보유하는 국방관련기관 및 방산업체는 모두 그림 2의 방위산업기술 보호체계를 갖추어야 한다.

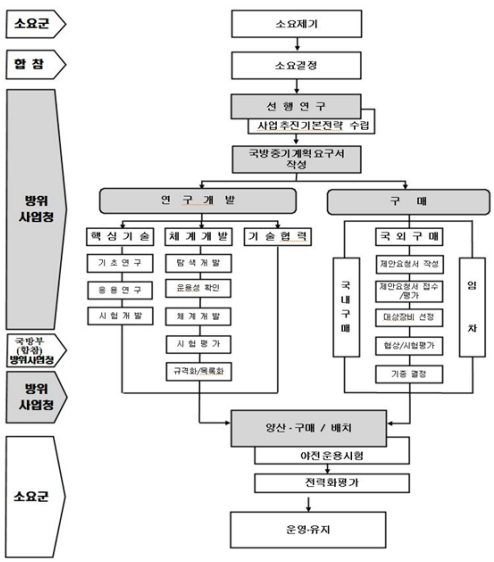
Ⅲ. 방산보안 2.0 시대

앞에서 기술한 바와 같이 방산보안은 1960년대부터 오랜기간 제도적으로 운용되어 왔으나 방위산업기술보호법의 시행과 더불어 법, 제도가 변화하고 정보통신 등의 기술 발달로 인해 방산보안 환경이 크게 변화하고 있다. 이에 본 논문에서는 방위산업기술보호법 이후를 방산보안 2.0 시대로 규정하였고, 시대 별 주요 특징을 정의하고 향후 과제를 논의한다.

3.1. 국방 획득 과정에서 보호 대상의 확대

방산보안 1.0 시대에는 국방 획득 과정에서 보호 대상이 군사기밀보호법에 따른 군사기밀 위주였다면 2.0 시대는 방위산업기술보호법에 따른 방위산업기술로 확대된다. 국방 획득이란 군수품(방산물자)을 구매하여 조달하거나 연구개발·생산하여 조달하는 것을 말하며 그림 3과 같은 방위력개선사업 절차로 수행된다[6,7]. 군수품 획득 절차는 일반적으로 군수품을 사용할 소요군의 소요제기로 시작하며 합참이 소요를 결정하면 방위사업청을 통해 연구개발 또는 구매하여 획득하게 되고 소요군에서 전력화하고 운영·유지 및 폐기하는 단계를 갖는다. 이러한 획득 과정에서 무기체계의 작전요구성능(ROC: Required Operational Capability) 등 군사기밀이 생산·유통될 수 있다.

방위산업은 군에 방산물자를 조달하기 위해 존재하며 방산업체는 방산물자의 연구개발 및 생산 과정에서 군의 군사기밀을 취급하게 되므로 방위사업법과 방위산업보안업무훈령에 의한 보안체계를 갖추고 있다.

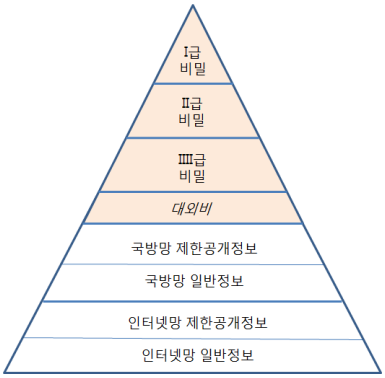


〔그림 3〕 국방 획득 체계 (출처: 방위사업관리규정)

새로 제정된 방위산업기술보호법은 방위산업기술을 보유하거나 연구개발하는 곳을 법의 대상기관으로 정하고 있다. 이에 따라 국방 획득 과정에서 방위산업기술을 보유하는 국가기관(방위사업청, 국방기술품질원, 국방과학연구소, 각군 등), 방산업체 등은 방위산업기술 보호체계를 구축해야 한다.

보호대상이 방위산업기술로 확대됨에 따라 국가가 보호할 방위산업기술의 식별이 요구되는데 현재는 방산업체가 보유하고 있는 방위산업기술의 식별이 진행 중이다. 향후에는 소요 및 연구개발과제(무기체계, 핵심기술) 기획 단계에서 무기체계 및 작전 성능에 핵심적 영향을 주는 방위산업기술을 식별하고 국방과학연구소, 방산업체 등이 연구개발하는 과정에서 기술을 보호할 수 있도록 하는 체계를 갖추어야 할 것이다. 획득 체계에서 방위산업기술 정보를 보유 또는 접근하는 각 군도 방위산업기술 보호 인식을 제고해야 하고 이를 위한 교육이 요구된다.

또한, 국방과학기술 정보의 분류체계를 정립하여 방위산업기술 정보의 분류체계가 정립되어야 한다. 국방과학기술 정보 중 비밀과제에서 생산되는 정보는 군사기밀보호법 등 관련 법규에 따른 비밀로 분류되어야 하며, 비밀이 아닌 정보는 보호등급을 부여하여 보호해야 한다. 국방과학기술 정보 중 비밀이 아닌 정보는 국방기술정보통합서비스(DTiMS: Defense Technology InforMation Service)를 통해 공개하는데 보호등급을 부여하여 공개범위를 제한해야 한다. 그림 4는 국방과학기술 정보의 등급 분류를 보여준다. 국방과학기술 정보의 분류 체계는 표준으로 만들어 대상기관이 통일된 분류지침에 따라 정보를 분류하고 적절하게 등급을 표시하여 보호하도록 해야한다.



〔그림 4〕 국방과학기술 정보의 등급 분류

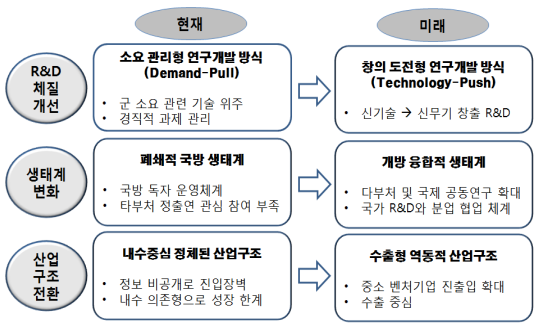
3.2. 국방산업 육성과 대상 기관의 확대

방산보안 1.0 시대에는 대상기관이 방산업체 위주였다면 2.0 시대는 대상기관이 벤처 중소기업을 포함한 일반업체, 대학, 연구기관 등으로 크게 확대된다.

방위산업은 군 소요 관련 기술 개발을 위주로 내수의존형으로 성장해왔다. 최근 인공지능, 빅데이터, 초연결 네트워크 등 4차 산업혁명 기반 신기술의 발전으로 전쟁 패러다임이 변화하고 있는데 현재 방위산업 체계로는 이러한 변화에 대응이 곤란하다. 이에 따라, 국방부는 최근 국방산업진흥회의를 개최하고 그림 5와 같은 '과학기술 기반 국방산업' 육성 계획을 발표한 바 있다[8]. 본 계획에 의하면 첫째, 국방 연구개발을 소요관리형 연구개발 방식에서 창의도전형 연구개발 방식으로 체질 개선하고 둘째, 폐쇄적 국방 생태계를 다부처 및 국제 공동연구 등 개방 융합적 생태계로 개선하고 셋째, 내수 중심 정체된 산업구조를 수출형 역동적 산업구조로 전환하는 한편 중소 벤처기업이 신기술을 이용하여 방위산업으로 쉽게 진출입하도록 지원할 계획이다. 이를 위해 '방위산업진흥법(가칭)'과 '국방과학기술혁신촉진법(가칭)'을 제정할 계획이다.

이러한 과학기술 기반 국방산업 육성 계획에 따라 벤처업체, 대학, 연구소 등에서 개발한 4차 산업혁명의 신기술을 이용하여 첨단 신무기체계 개발이 촉진될 것이며 이 과정에서 국가안보를 위한 방위산업기술을 식별하고 국외로 유출되지 않도록 보호해야 한다.

군 소요에 의한 연구개발이 아니라 업체, 대학, 연구소 등이 자체 개발한 첨단 신기술이 창의적으로 무기체계에 활용되고 국방산업을 진흥하기 위해서는 국방과학기술의 소유권을 국가가 아닌 기술을 개발한 곳이 갖도록 해야 한다. 이때 업체 등이 자체 연구개발한 기술에



〔그림 5〕 과학기술 기반 국방산업 육성 방향

대해 지식재산권(특허 등), 영업비밀 및 방위산업기술의 분류 및 관리 체계가 정립되어야 한다.

일반업체, 대학 등에서 연구개발한 신기술의 무기체계 적용은 결국 체계업체인 방산업체에서 하게 된다. 방산업체는 협력업체와 상생 및 동반성장하는 생태계를 구축해야 하고 보안체계가 미흡한 협력업체의 보안업무를 지원하여 상호 보유하게 될 방위산업기술이 유출되지 않도록 해야한다.

3.3. 사이버 보안의 중요성 증대

방산보안 1.0 시대에는 문서보안, 시설 및 인원보안과 같은 물리적 보안이 중요했으나 정보통신기술의 발전에 따라 기술적 보안의 중요성이 커지고있다. 최근인 2017년 방산업체는 의무적으로 물리적 망분리 시스템을 구축하였다. 앞으로 스마트 공장, 모바일, 사물인터넷, 인공지능 등의 발전으로 업무 환경이 정보시스템으로 더욱 고도화될 것이다. 정보 기기를 이용한 내부자의 기술 유출, 사이버 공격을 통한 외부자의 기술 유출이 자행되고 있어 방산보안 2.0 시대에는 사이버 보안의 중요성이 확대된다.

방산보안 1.0 시대에 보호대상인 군사기밀은 네트워크와 단절된 PC에서 생산되고 비밀합동보관소에 보관되었지만 방산보안 2.0 시대에는 방위산업기술 자료가 네트워크와 연결된 연구원 PC에서 취급된다. 방산업체는 의무적으로 물리적 망분리 시스템을 구축하여 업무망과 인터넷망이 분리되어 방위산업기술 자료를 보호할 수 있지만, 그 외 대상기관은 망분리가 의무가 아니므로 인터넷을 통한 자료 유출이 용이하다. 보호구역의 정보보호 시스템 구축, 자료의 보호등급 별 접근제한, 외부반출 및 유통 간 보호대책이 요구된다.

향후에도 정보통신의 발전에 따라 물리 공간과 사이버 공간이 융합되고 사이버 공격 기술이 다양하게 발전할 것으로 예상되며 이를 방어하기 위한 정보보호 시스템 구축과 운용 비용은 꾸준히 증가할 수 밖에 없다. 대상기관에 요구되는 정보보호 시스템, 보안관제 등에 국가의 적극적인 예산 지원이 절실하다.

보안관제의 경우, 대상기관이 자체 운영하기에는 예산 확보와 고도의 전문인력이 요구되기 때문에 제한되며 외부 용역업체에 맡기는 것은 국가안보와 관련된 민감한 국방 정보가 유통될 수 있기에 바람직하지 않으므로 방산 정보공유분석센터(ISAC: Information Sharing and Analysis Center) 구축을 검토할 필요가 있다. 방산 ISAC은 통합보안관제를 제공하며 사이버 침해 위협을 수집 및 분석하고 신속하게 회원기관에 전파함으로써 효율적인 공동대응체계를 구축할 수 있다. 또한, 모의침투, 취약점 분석 등 전문적인 사이버 보안 서비스를 제공한다.

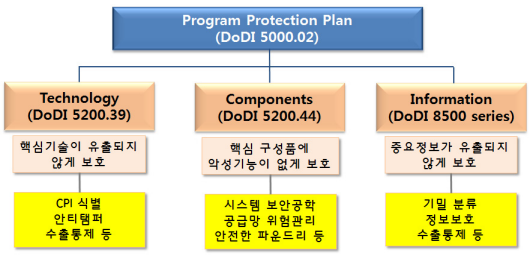
3.4. 무기체계 보안의 대두

방산보안 1.0 시대는 무기체계의 보안을 거의 다루지 않았으나 2.0 시대는 방위산업기술보호법에 의해 무기체계에 구현된 방위산업기술에 대해 기술보호기법 적용이 요구된다.

국방 선진국인 미국은 전장에서 손실되는 무기체계 또는 수출한 무기체계에 대해 적 또는 수입국에서 역공학을 이용 핵심기술이 탈취되는 것을 방지하기 위해 기술보호기법인 안티 탬퍼(anti-tamper) 기술을 적용하고 있다. 이를 위해 그림 6과 같은 프로그램 보호 계획(PPP: Program Protection Plan) 제도를 수립하여 무기체계 획득 체계에 안티 탬퍼, 시스템 보안 공학을 내재화하고 무기체계의 핵심기술을 보호하고 있다[9-12].

무기체계는 컴퓨터가 통제하는 임베디드 시스템화되고 네트워크 통신망에 연결되고 있어 사이버 공격에 노출되고 있다. 사이버 공격으로 무기체계를 장악하게 되면 무기체계의 소프트웨어 핵심기술 등을 유출해갈 수 있다. 사이버 공격은 보통 임베디드 소프트웨어의 취약점을 이용하게 되므로 시스템 보안 공학을 통해 취약점이 없도록 설계하고 시험평가를 수행한다. 또한, 무기체계의 공급망을 통한 사이버 공격에 대비하는 보호체계도 갖추어야 한다.

우리나라는 아직 무기체계의 기술보호기법 적용을 위한 제도가 정립되어 있지 않다[11,12]. 향후 법제 수



〔그림 6〕 미국 국방부의 프로그램 보호 계획

립, 기술 개발이 요구되며 이를 위한 전문 인력양성과 연구개발 지원이 필요하다.

3.5. 개방적 제도 운영과 지원

방산보안 1.0 시대는 군 기관의 통제, 감독을 통한 폐쇄적 제도로 운영되었다면 2.0 시대는 기술보호와 관련된 다양한 기관의 협력 및 지원을 통한 개방적 제도로 운영된다.

방산보안 1.0 시대에는 군사안보지원사령부(구 기무사령부)가 방산업체의 보안감사 및 보안측정, 보안교육, 신원조사, 군사기밀 유출 수사 등을 전담하였다. 군의 특성상 폐쇄적으로 운영해왔고 학계를 포함한 민간 기관과의 정보공유 및 교류가 거의 없었다.

방산보안 2.0 시대에서 방위산업기술보호법은 방위사업청이 주무 기관이므로 방위사업청과 군사안보지원사령부는 긴밀한 협력을 통한 대상기관의 지원이 필요하다. 특히, 기존 법규와 방위산업기술보호법의 중복 조항으로 인해 대상기관의 보안 업무가 가중되지 않도록 세심한 정책 조율 및 법령의 개정 등이 요구된다. 또한, 방위산업의 진흥을 위한 방산보안 정책 수립이 요구되며 이를 위해 기관 지향적 통제 정책이 아닌 현장 지향적 서비스 정책이 되어야 한다.

또한, 방위사업청, 군사안보지원사령부, 기술보호 유관기관인 국가정보원 산업기밀보호센터, 경찰청 산업기술유출수사대 등은 공조 및 협력을 통해 대상기관에 대한 지원이 필요하다.

나아가 유관 기관들은 대학(원), 학회, 연구회 등 학계와의 협력과 지원을 통해 방산보안 전문인력 양성, 관련기술 연구개발을 지원해야 한다. 민간 기관과의 정보공유, 상호교류 및 지원을 통해 학술연구 및 연구개발을 촉진함으로써 우리나라 방산보안 분야가 국제적 수준으로 발전할 수 있도록 개방적 선진 방산보안 지원 제도 구축이 필요하다.

Ⅳ. 결 론

이상으로 방산보안 2.0 시대의 주요 특징과 발전 방향을 살펴보았다. 본 논문에서 기술한 방산보안 시대와 특징은 앞으로 심도있는 논의가 필요하며 연구를 통해 구체적으로 정립할 필요가 있다. 방산보안은 국가 안보와 직결되며 방산 수출에 기여하여 국가 경제에도 이바지하는 중요한 분야로서 국방, 국제정치, 공학, 법학, 경영, 행정, 정보보호 등 다양한 분야를 망라하는 종합 학문이다. 본 논문을 통해 다양한 분야의 전문가들이 방산보안을 연구하여 국가 안보와 경제에 이바지할 수 있기를 기대한다.

참 고 문 헌

[1] 한국방위산업학회, “방위사업 40년 끝없는 도전의 역사”, 플래닛미디어, Mar. 2015.
[2] 채우석, “황금알을 낳는 최첨단 방위산업 삼성은 왜 포기했나”, 윈윈미디어, Oct. 2018.
[3] 국방부 훈령, “방위산업보안업무훈령”, 2018. 2
[4] 법률 제15052호 “방위산업기술보호법”, 2017. 11
[5] 법률 제15051호 “방위사업법”, 2017. 11
[6] 방위사업청 훈령, “방위사업관리규정”, 2018. 10
[7] 육군본부, “2017년 방위력개선업무 실무지침서”, 2017. 1
[8] 국방부-방사청 공동보도자료, “국방산업진흥회의 개최”, 2018. 9.14.
[9] DoD Instruction 5200.39, “Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)”, May. 2015.
[10] DoD Directive 5200.47E, “Anti-Tamper”, Sep. 2015.
[11] 류연승, “선진국 방산기술보호 사례 및 적용 방안”, 제15회 국방정보보호 컨퍼런스, Nov. 2017.
[12] 류연승, “무기체계 소프트웨어 핵심기술 보호 방안”, 2018 획득업무 발전 컨퍼런스, Sep. 2018.

〈저 자 소 개〉

류 연 승 (Yeonseung Ryu)
종신회원

1990년 2월 : 서울대학교 계산통계학과 학사
1992년 2월 : 서울대학교 계산통계학과 전산과학 석사
1996년 8월 : 서울대학교 계산통계학과 전산과학 박사
2003년 3월~현재 : 명지대학교 컴퓨터공학과 교수
2014년 9월~현재 : 명지대학교 대학원 융합보안학과 교수
2015년 3월~현재 : 명지대학교 대학원 보안경영공학과 교수
관심분야 : 방산보안, 무기체계보안, 보안경영